

Design and simulation verification of a fault escalation and lockout control system for solar charge controllers

C.H. Udeji¹, K.C. Obute¹, Dr. Olufolahan Oduyemi²

¹Department of Electrical Engineering, Nnamdi Azikiwe University, Awka, Nigeria

² Cummins inc, Columbus Indiana, USA

Corresponding Author - K.C. Obute

Abstract

The charge controller of a departmental hybrid solar power system is part of a commercial hybrid inverter, whose documentation lists fault codes but does not disclose their trigger thresholds and escalation rules. In this study, a finite state machine for fault escalation and lockout of this charge controller is proposed. The Moore machine was implemented in Verilog-2001 register-transfer-level (RTL) style code with four states (Normal, Warning, Fault, Lockout) and four faults. Overcurrent, overcharge, and overtemperature faults each represent constraints on continuous values (current, voltage, temperature); each has a warning input, an alarm input, and an integrator counter with a threshold reflecting urgency (example values: 3, 7, and 15 clock cycles). Overcurrent escalates fastest and overtemperature slowest. Reverse polarity, a binary condition without thresholds, forces immediate lockout from any state. Once locked out, all active faults are recorded for diagnostics, and leaving requires a manual reset, which is refused while any fault or warning persists. For verification, a self-checking testbench of 33 scenarios, with expected results derived from the specification before code review, was constructed. It passed in full and exercised all 16 specified transitions. Run unchanged against a design with one intentionally altered threshold, it detected the alteration. Verification was by simulation only; no hardware was built.

Keywords: Finite state machine; fault escalation; solar charge controller; lockout; functional verification

Date of Submission: 15-10-2026

Date of Acceptance: 28-10-2026

I. Introduction

Within a solar hybrid power generation system, the role of the charge controller is to regulate energy transfer between the photovoltaic (PV) panel array, batteries, and loads. Four faults are of particular concern. Overcharge deteriorates the battery cells and can lead to thermal runaway in lithium-ion cells. For example, a study by Wei et al. (2022) compares the effects of three abuse methods, and shows that overcharge results in the highest levels of cell damage. Overcurrent stresses switching devices and wiring, overtemperature endangers both electronics and cells, and reverse battery polarity, typically introduced during installation, can damage polarity-sensitive semiconductor components once power is applied.

The charge controller used in the departmental cohort hybrid solar power installation, a collaborative project with one student team responsible for each subsystem, is integrated within a commercially available hybrid inverter, the itel IPV-6K48UPRO (6 kW, 48 V). The official user manual contains fault codes for overcurrent, overcharge, and overtemperature conditions, with separate overtemperature codes for five internal circuits. No information is provided about the fault threshold conditions and their timing and escalation strategies (Table 1; itel Energy, n.d., pp. 49–52). There is also no fault code related to battery polarity reversal. This lack of detail limits further investigation and reuse, because the documentation does not explain how the unit separates transient from persistent faults, records the cause of a shutdown, or governs recovery. This is a documentation limit, not a claimed defect of the unit. The urgency level of different hazards is likely to vary; for instance, overcurrent is generally expected to threaten switching devices quickly while overtemperature develops more slowly because of thermal mass. A single response policy is therefore unlikely to suit all four.

Table 1
Fault categories of this work against the fault codes in the itel
IPV-6K48UPRO user guide

Category	itel code	Documented description
----------	-----------	------------------------

Overcurrent	11, 12, 31, 35, 36, 43	Over current or surge detected by software (11) and hardware (12); over current in converter circuits (31, 35, 36) and at the PV port (43)
Overcharge	30	Excessive battery voltage
Overtemperature	51–55	Separate codes for five internal circuit sections
Reverse polarity	None	No code for reversed battery polarity; codes 17 and 23 concern AC wiring

Published designs leave a similar gap (see Table 2). Amin et al. (2009) use a persistence count of nine cycles, with the voltage held at or above its set-point, to gate equalization in a PIC16F877A microcontroller-based charger, while load disconnection is decided from temperature and voltage inputs. They report no test results. Raghavendra and Padmavathi (2018) apply a fixed reference comparator to stop the charging process in a one-cell lithium-ion charger. They add a prevention mechanism in a three-cell version of this charger by including a P-channel metal–oxide–semiconductor field-effect transistor (MOSFET) circuit so that a reversed connection is never energized. This design was tested on hardware. Neither study keeps a record of the disconnection cause beyond a light-emitting diode (LED)

Table 2

Approach	Timing differentiation by fault type	Fault-cause retention	Verification
Amin et al. (2009)	Not differentiated; one persistence count gates one charging-stage decision	Status LEDs show the current mode only	Logic and state diagram documented; no test results reported
Raghavendra and Padmavathi (2018)	Not differentiated; fixed-reference comparator cut-off	None; a reversed connection is prevented, not logged	Hardware prototype with measured charge and discharge curves
Maheshwari et al. (2014)	Continuous inverse-time curve (IEEE C37.112), graded by overcurrent magnitude, one fault type	Not addressed; values sent live over a link only	Hardware; 360 km transmission-line simulator
Shehata et al. (2004a,b)	A separate mechanism per category (3 in the FPGA design, 6 in the microcontroller variant)	Microcontroller variant keeps the last three trips in non-volatile memory (entry format not described); FPGA variant: LED indication	Hardware prototypes with measured accuracy
Texas Instruments (2022), BQ76920 family	A programmable delay for each protection (overcurrent and short circuit in discharge, over- and undervoltage)	Status flags latched until the host clears them	Commercial device; specified in its data sheet
This work	One repeated counter-and-threshold independent per category vector through values from the specification	Latch holding the full simultaneous fault Lockout self-checking testbench, and graded by urgency	Simulation only: directed structure, expected

Fault protection approaches compared with this work

status indicator. In protective relay systems, Maheshwari et al. (2014) implemented Institute of Electrical and Electronics Engineers (IEEE) Std C37.112 inverse-time overcurrent characteristics for protection on a field-programmable gate array (FPGA) board but only for a single quantity. Shehata et al. (2004a,b) developed an FPGA design and a microcontroller variant where each type of fault condition (e.g., overcurrent, phase loss, and

This work claims no conformance to the relevant industry standards, such as IEC 61511-1 (International Electrotechnical Commission), ANSI/ISA-18.2 (American

National Standards Institute and International Society of Automation), or IEEE C37.2, but it uses several conventions that reflect important principles stated within the standards. IEC 61511-1 (IEC, 2016) emphasizes that operation should not resume before the removal of a detected hazard is verified, a principle the permissive reset follows. The four-level alert structure draws on the principles of the alarm-priority scheme in ANSI/ISA-18.2 (ISA, 2016). The finite state machine (FSM) follows IEEE Std C37.2 (IEEE, 2008) in using device numbers 86 and 30 for lockout and annunciator. IEC 61508 (IEC, 2010a) defines general functional safety requirements and IEC 62109-1

(IEC, 2010b) defines product safety requirements for locked rotor, among others) had its own purpose-built mechanism. Only the microcontroller variant stores information regarding the last three trips, although it remains unclear whether a single log corresponds to multiple faults occurring concurrently. Closer similarities exist in the functions of commercial battery-protection devices. For example, the Texas Instruments BQ76920 family has programmable delays for discharge-overcurrent, discharge-short-circuit, overvoltage, and undervoltage protection, as well as status flags that are latched until cleared by the host (Texas Instruments, 2022). photovoltaic power converters; conformance to neither is claimed.

Contributions of this work include:

- (i) a synchronous FSM in Moore style, which handles faults according to their category characteristics;
- (ii) three separate integration counters with urgency-ordered threshold levels;
- (iii) a Lockout state activated either through sustained escalation of an alarm in Fault, or instantaneously by reverse polarity, and left only through a global reset or the user-triggered permissive reset;
- (iv) a latch register that captures a record of every fault active when the Lockout state is entered; and
- (v) a directed self-checking verification approach that compares observed results against expected behavior inferred directly from specifications rather than RTL implementation, and was itself checked by one deliberate threshold mutation.

The fault escalation and lockout subsystem processes faults but does not sense them directly; it accepts as input binary pre-thresholded fault warnings and alarms from sensing circuits along with reverse polarity status, assumed to come from an independently protected detection circuit. Verification is performed by simulation on an abstract clock. Counter threshold constants reflect timing relationships, not specific absolute times.

II. Materials and methods

(GNU Image Manipulation Program) ToolKit (GTK). As shown in Fig. 1, the scope of the presented designs excludes the sensing logic circuits generating inputs to the module and a relay controlled by the trip output. Inputs include: clock signal, synchronous active-high reset signal, manual_reset signal, warnings and alarms of overcharge (ovc), overcurrent (oc), and overtemperature (ot) conditions, and finally, rev_pol representing reverse polarity condition without any corresponding warning level.

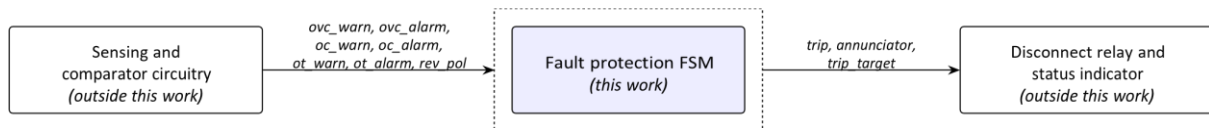


Fig. 1. Scope of the fault protection FSM within the cohort hybrid solar power system (dashed boundary).

Outputs include: alert_level providing the current twobit encoded state value from “00 Normal” to “11 Lockout”, annunciator (high in every state except Normal), trip signal

2.1 Materials

In this paper, the designs are specified in Verilog-2001 style with .sv file extension¹ where the states were defined as named parameters. The designs were simulated with Icarus Verilog, an open-source simulator, and the waveforms, saved in value change dump (.vcd) format, were examined in GTKWave, a viewer built on the GIMP

2.2 Methods

2.2.1. State machine and transitions

The design realizes a synchronous Moore-style machine where the trip and annunciator outputs triggering safety hardware depend exclusively on the current state value, unlike Mealy machines, which allow input-triggered output glitches (trip_target outside Lockout is a deliberate exception, Section 2.2.4). The state value uses two bits in binary encoding, and alert_level output wire was directly connected to it. Reset is synchronous, so the state changes only at clock edges. The design structure consists of a clocked register storing the state value, combinational logic computing the next state according to the case statement, combinational assignments setting the trip and annunciator outputs from the state value and trip_target from the alarm inputs and the latch, and dedicated clocked circuits implementing each of the three independent counters as well as a latch for trip_target. Following the reset applies from any state, including Lockout.

high only in Lockout state used for actuating the disconnection relay, and a four-bit signal called trip_target (live outside Lockout) storing the reasons why Lockout state was initiated (bits 0–3 stand for overcurrent, overcharge, overtemperature, and reverse polarity). All signals are active-high and level-sensitive, sampled at each clock edge.

device numbers of IEEE Std C37.2, Lockout refers to device 86, the lockout relay that keeps equipment disconnected from the power supply until it is reset manually. Annunciator output corresponds to device 30.

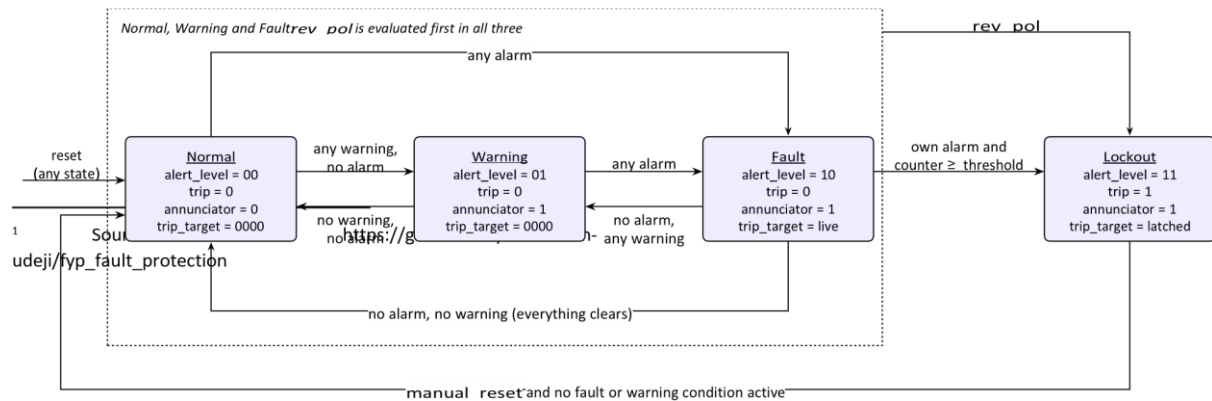


Fig. 2. State diagram of the fault protection FSM. Each state holds when none of its exit conditions is met (the “else” rows of Table 3);

Fig. 2 depicts the state transition diagram, while Table 3 contains the full transition table including the scenarios that exercise each transition. Priorities among conditions from highest to lowest are reverse polarity, alarm, warning. To enter Lockout from Fault, the respective alarm must be true, and the associated counter, as stored at the start of the current cycle, must have reached the threshold. The counter therefore still equals the threshold in the last cycle spent in Fault, and Lockout begins at the next edge.

2.2.2. Fault handling and integration counters

The system classifies faults into three categories (overcurrent, overcharge, and overtemperature), each having associated warning and alarm levels as well as integration counters. Such a counter is incremented within every cycle during which the FSM is in the Fault state and the associated alarm is high, and it is cleared in any cycle during which the FSM is not in Fault or the alarm is low, and on reset. A single common counter was rejected because the integration window must vary with the urgency of each hazard category. Reverse polarity is a wiring condition with no warning level; due to immediate risks to semiconductor safety upon applying power in such circumstances, the presence of the condition is assessed first in every state and directly leads

Table 3

FSM state transition table, with the scenarios that exercise each transition

No.	From	Condition	To	Exercised by scenario
1	Normal	any warning, no alarm	Warning	2
2	Normal	any alarm	Fault	4; 21 (direct, no warning)
3	Normal	rev_pol	Lockout	27
4	Normal	nothing active	Normal	1
5	Warning	no warning, no alarm	Normal	3
6	Warning	any alarm	Fault	20
7	Warning	rev_pol	Lockout	28
8	Warning	warn condition persists	Warning	19
9	Fault	own alarm, own counter ≥ threshold	Lockout	6; 10; 13; 26
10	Fault	rev_pol	Lockout	29
11	Fault	no alarm, any warning	Warning	16
12	Fault	no alarm, no warning	Normal	23
13	Fault	alarm persists, counter test not yet passed at cycle start	Fault	5; 22
14	Lockout	manual_reset, nothing currently active	Normal	32
15	Lockout	anything else	Lockout	31
16	Any state	reset (unconditional override)	Normal	7

2.2.3. Lockout and permissive manual reset

Lockout can be triggered through escalation, where a counter reaches its threshold value, or by reverse polarity. It can be exited by either a global reset signal or a successful manual_reset, but not otherwise. Global reset is an unconditional override meant for power-up and hardware resets, when all previous states should be

discarded as untrusted. `manual_reset` signifies a claim made by the operator that the issue triggering the lockout has been corrected. This claim will only be accepted if no warnings or alarms are detected across the four categories of conditions. As `rev_pol` is an active condition, its simultaneous occurrence alongside `manual_reset` keeps the FSM in the Lockout state.

the FSM into the Lockout state, even when another alarm is active.

The thresholds are 3 cycles for overcurrent, 7 for overcharge, and 15 for overtemperature (Table 4). They are configurable and meant to differentiate timing, not calibrated to any measured physical parameter. Each threshold after the first equals twice the previous one plus one, to keep three different fault propagation speeds distinguishable during simulations. A counter can increment once more on the edge when the FSM leaves Fault, so each peak exceeds its threshold by one. The highest peak is 16 counts (the overtemperature case), so all three counters have five-bit widths. Starting to count on the rising edge when an alarm first appears entails spending one edge entering the Fault state and one more edge acting on the collected counts, making the total required edges two greater than each of the above threshold values (5, 9, and 17 edges for overcurrent, overcharge, and overtemperature). A threshold is not a latency.

2.2.4. Trip-target latch

This latch retains the four-bit `trip_target` record, representing the digital counterpart of flags used in protective relays. A multiplexer controlled by the Lockout state indication selects the source of the output. Outside Lockout, it selects the combinational path carrying the current alarm statuses, and bit 3 corresponds to the `rev_pol` status. At the clock edge that starts the Lockout state, the register captures this multiplexer output. The multiplexer then keeps outputting the register content for the whole of Lockout, so later input changes cannot alter the record. The latch is cleared only when Lockout is left. Live tracking outside Lockout is deliberate, since this output is diagnostic and not part of the protective path. If several alarms are active when one counter reaches its threshold, the latch keeps them all.

2.2.5. Verification approach

Directed self-checking tests were adopted instead of constrained random stimuli (Bergeron, 2003). Given the manageable structural state space (four states, three threshold levels, and a bypass), the full enumeration is feasible by manual inspection. Transitions were taken from Table 3 and threshold boundaries from Section 2.2.2. The much larger space of input sequences over time cannot be covered by the 33 scenarios performed (see Section 4). Expected outputs were derived from the transition table before the actual RTL behavior was observed, so the testbench does not repeat any errors made in the design. A scenario applies stimulus to the inputs and waits one time unit before making four comparisons of `alert_level`, `trip`, `annunciator`, and `trip_target` (the clock period of 10 time units is a simulator convention, unrelated to the threshold bounds). An anomaly generates an error message specifying the failed scenario and increments the error count without terminating execution. The scenarios cover direct and two-step paths between the first three states, the exact boundary of each counter and the independence of the counters, accepted and refused manual resets, reverse polarity from three states, latching of several faults, and a pulse falling between clock edges.

The mutation check involved one change (setting `OC_THRESHOLD=5`) applied solely to the design; the whole suite was then re-run and the constant restored. Timing, power consumption, and synthesis analyses were not performed; the design module consists of synthesizable constructs exclusively, whereas the testbench, as usual, does not.

III. Results

All 33 scenarios passed without errors when simulated locally using Icarus Verilog as well as on electronic design automation (EDA) Playground online simulation service.

While the absence of errors in these two settings rules out artifacts stemming from differences in installations (both runs use the same simulator engine), this result fails to establish cross-simulator reproducibility. Scenarios are numbered in the order in which the testbench applies them. Table 3 correlates scenarios with the corresponding state transitions,

Table 5 gives the main observation for each scenario, while Figs. 3–9 show waveform diagrams.

3.1 Escalation and threshold crossing

Fig. 3 shows the essential escalation path, in which `oc_warn` transitions the FSM to the Warning state, then back to Nor-

Table 4

Fault-integration counter thresholds and observed peaks `mal` on its release (scenarios 1–3). In Fig. 4, `oc_alarm` moves the FSM to Fault state with `trip_target` live at 0001. `oc_counter` increments to 1, 2 and 3 while the FSM is

in Fault, and it shows the threshold value of 3 in the last cycle before Lockout (scenario 5). At the next clock edge, the FSM transitions to Lockout state, trip goes high, the latch captures 0001, and oc_counter equals 4 (scenario 6). Lockout begins on the fifth clock edge at which oc_alarm is sampled high, and a global reset then clears all outputs (scenario 7). Overcharge and overtemperature behave the same way, peaking at 8 and 16, one above each threshold (scenarios 8–13).

3.2 Counter independence and alternative paths

Replacing oc_alarm with ovc_alarm clears oc_counter at once (from 2 to 0), and ovc_counter then runs alone, reaching 7 in the Fault state and showing 8 when Lockout starts (scenarios 14–15, Fig. 5). Clearing the alarm early, while a warning remains, triggers a return to Warning and a

Fault category	Threshold (cycles)	Observed counter peak	Speed to Lockout
Overcurrent	3	4	Fastest
Overcharge	7	8	Intermediate
Overtemperature	15	16	Slowest

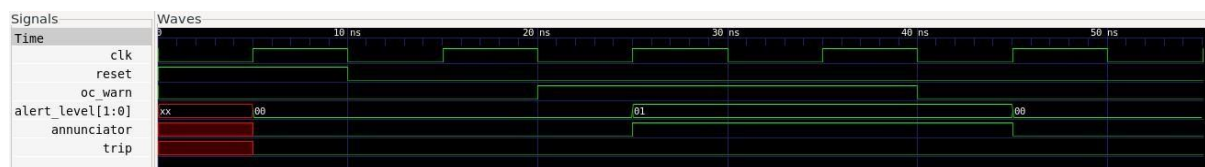


Fig. 3. Basic escalation (scenarios 1–3): oc_warn takes the FSM from Normal to Warning, and its release returns it.

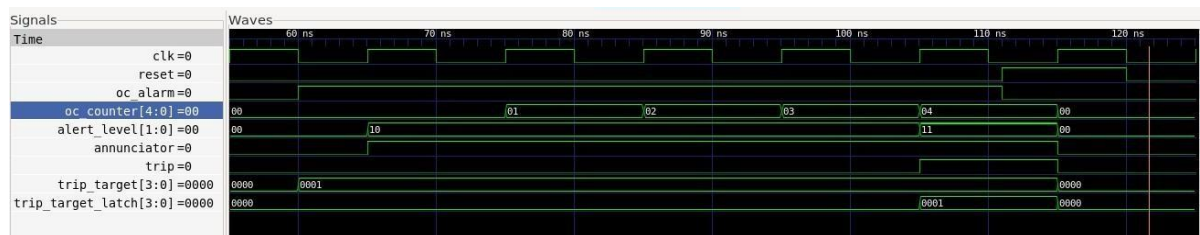


Fig. 4. Overcurrent integration (scenarios 4–7): oc_counter counts 1–3 in Fault; at the next edge Lockout begins, the counter reads 4 and the latch captures 0001; reset then clears all outputs.

further transition to Normal state instead of Lockout entered without a previous warning returns straight to (scenarios 16–17). The alert level jumps from 01 to 10 Normal when the alarm clears (scenarios 21–23); these when the alarm is asserted in the third clock cycle of a are two separate next-state branches. three-cycle Warning state (scenarios 18–20, Fig. 6). A Fault

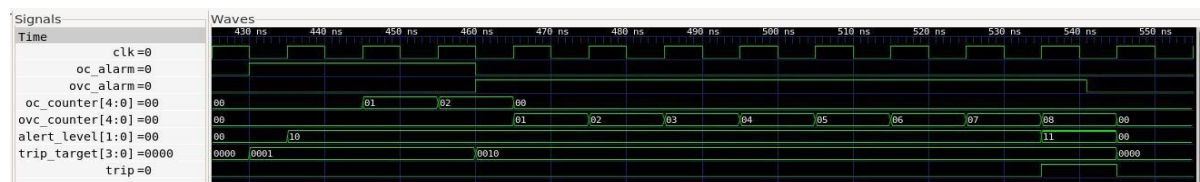


Fig. 5. Counter independence (scenarios 14–15): switching the alarm category clears oc_counter; ovc_counter reaches 7 in Fault and reads 8 as Lockout begins.

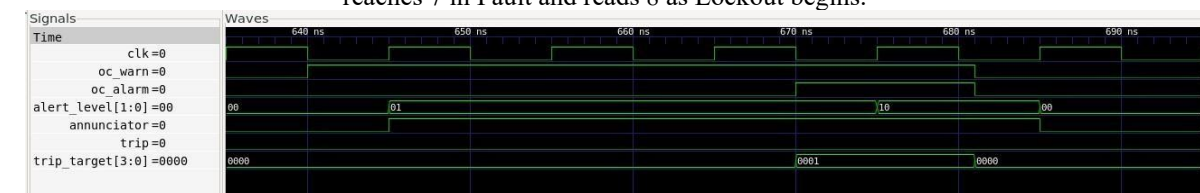


Fig. 6. Direct Warning-to-Fault transition (scenarios 18–20): alert_level goes from 01 to 10 with trip_target live at 0001.

3.3. Latch capture and reverse-polarity bypass

7). The reverse-polarity signal (rev_pol) sent the FSM to Lockout directly from Normal, from Warning, and part- With oc_alarm and ot_alarm both active, trip_target was live at 0101. When the faster overcurrent counter sent the way through a count in Fault (scenarios 27–29, Fig. 8); in

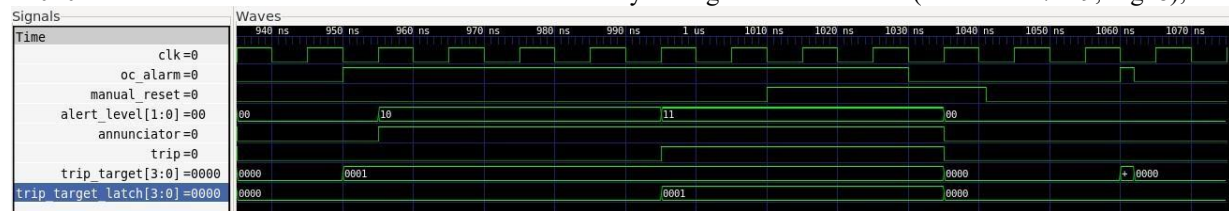


Fig. 9. Permissive reset and sampling (scenarios 30–33): manual_reset is refused while oc_alarm is active and accepted after it

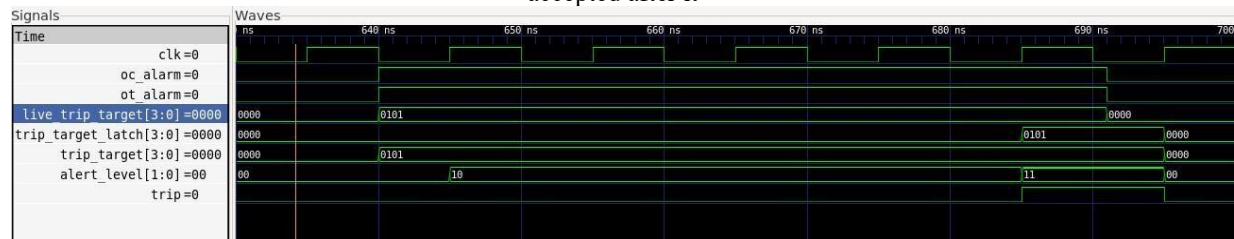


Fig. 7. Multi-fault latch (scenarios 24–26): both alarm bits (0101) are captured when Lockout begins.

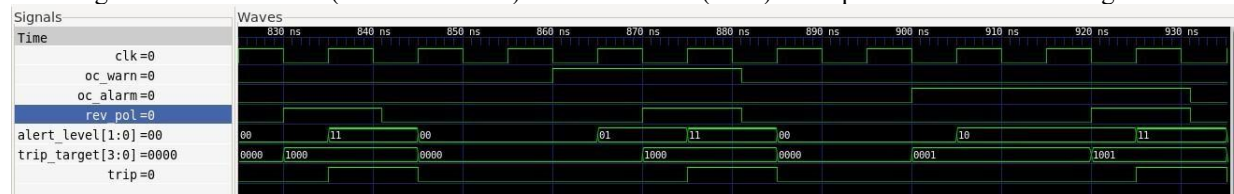


Fig. 8. Reverse-polarity bypass (scenarios 27–29): immediate Lockout from Normal (latch 1000), Warning (1000) and mid-count in Fault (1001).

FSM to Lockout, the latch kept both bits even though only that counter reached its threshold (scenarios 24–26, Fig.

3.4. Permissive reset and sampling

After an overcurrent lockout (scenario 30), manual_reset was ignored as long as oc_alarm stayed active (scenario the first two cases the latch held 1000, and in the last it held 1001 because oc_alarm was still active. 31) and accepted after the clearance of oc_alarm, bringing the FSM back to Normal state and clearing the latch (scenario 32, Fig. 9). A 2-time-unit pulse on oc_alarm that began and ended between two rising clock edges was never sampled (scenario 33); a pulse straddling the clock edge would be sampled in the same way as any other input.

clears; a 2-time-unit pulse between clock edges is not sampled.

3.5. Mutation check

With OC_THRESHOLD set to 5, the unmodified testbench failed in three scenarios (6, 26, and 30), expecting Lockout

(alert_level 11, trip 1) and observing Fault (10, 0) because the counter value of 4 no longer met the threshold. Restoring 3 returned 33 of 33 passes.

3.6. Coverage and register count

The scenarios exercised all 16 transitions defined in Table 3. The clocked registers used in this implementation comprised 21 bits: two for the state register, five for every counter, and four for the latch (while next_state logic was combinational).

Table 5

No.	Scenario	Key observed value
1	Reset releases the design into Normal	alert_level = 00
2	Overcurrent warning raises Warning	alert_level = 01
3	Warning released, return to Normal	alert_level = 00
4	Overcurrent alarm raises Fault	trip_target = 0001 (live)
5	Overcurrent: Fault still held on the threshold cycle	oc_counter = 3

6	Overcurrent: Lockout on the next edge, cause latched	oc_counter = 4; latch = 0001
7	Global reset leaves Lockout	alert_level = 00
8	Overcharge alarm raises Fault	trip_target = 0010 (live)
9	Overcharge: Fault still held on the threshold cycle	ovc_counter = 7
10	Overcharge: Lockout on the next edge, cause latched	ovc_counter = 8; latch = 0010
11	Overtemperature alarm raises Fault	trip_target = 0100 (live)
12	Overtemperature: Fault still held on the threshold cycle	ot_counter = 15
13	Overtemperature: Lockout on the next edge, cause latched	ot_counter = 16; latch = 0100
14	Alarm category switched during Fault: old counter cleared	oc_counter = 0; Fault held
15	Overcharge alone reaches Lockout on its own schedule	ovc_counter = 8
16	Alarm clears before threshold while a warning remains	alert_level = 01; trip_target = 0000
17	Remaining warning clears	alert_level = 00
18	Overcurrent warning raised (set-up for direct entry)	alert_level = 01
19	Warning persists through a further clock edge	alert_level = 01 (held)
20	Alarm raised during Warning: direct entry to Fault	alert_level = 10; trip_target = 0001
21	Alarm raised from Normal with no warning: direct entry to Fault	alert_level = 10; trip_target = 0001
22	Fault held for one extra cycle	alert_level = 10 (held)
23	Alarm cleared: direct return from Fault to Normal	alert_level = 00; trip_target = 0000
24	Overcurrent and overtemperature alarms together	trip_target = 0101 (live)
25	Fault still held at overcurrent's threshold	oc_counter = 3
26	Faster overcurrent counter reaches Lockout, both causes latched	latch = 0101
27	Reverse polarity from Normal: immediate Lockout	latch = 1000
28	Reverse polarity from Warning: immediate Lockout	latch = 1000
29	Reverse polarity part-way through a count in Fault	latch = 1001
30	Lockout reached through overcurrent escalation	alert_level = 11; latch = 0001
31	Manual reset while the alarm is still active: refused	alert_level = 11 (held)
32	Manual reset after the alarm clears: accepted	alert_level = 00; latch = 0000
33	Pulse on the alarm input between clock edges	alert_level = 00 (unchanged)

Directed scenarios and their key observed values

IV. Discussion of results

For each implemented protection mechanism, the simulation tests confirm adherence to the corresponding specifications. For example, take the case (Fig. 5) when alarms alternate between categories. With a single shared counter, each category could stay below the threshold on its own while the shared count still triggers Lockout; separate percategory counters close this path by construction. The latch records the full fault vector, not only the fault whose counter crossed its threshold (Fig. 7). The reverse-polarity bypass overrides a count in progress and keeps whatever fault information was live (Fig. 8); this suits a wiring condition that requires instant action. The itel guide documents no automated response to reversed battery polarity (Table 1), and the bypass has not been tested against that unit. The permissive reset is unable to re-arm the system into a persistent hazardous condition

(Fig. 9).

Sampling has limits. As sampling takes place only at clock edges, any pulse falling fully between two edges would have no effect on the system states (scenario 33). This limitation should not be confused with noise rejection, since a disturbance aligned with the clock edge is still sampled as any other input, whereas an input pulse narrower than a clock interval would still be recorded if it crossed an edge. Rejection of brief alarms should rather be delegated to integration counters preventing such an alarm from becoming a Lockout condition. Asynchronous sensor signals would need additional synchronization hardware.

In contrast with the scheme of Amin et al. (2009), where one persistence count gates one charging decision, and the inverse-time protection applied by Maheshwari et al.

(2014) to a single quantity, per-category counters allow differentiated timing. Shehata et al. (2004a, 2004b) discriminate faults using separate mechanisms for each and, in the microcontroller variant, record trips. Here a single counter-and-threshold mechanism is repeated for every category, with a different threshold in each. In the proposed scheme all active alarms at the moment of trip are saved as a vector via the latch component, which the description of their trip memory does not state. The scheme by Raghavendra and Padmavathi (2018) prevents current flowing through a misconnection, whereas the bypass here escalates and records a reversal already detected; the two complement each other. None of the individual mechanisms is novel on its own (per-

category delay with status flags is known in some commercial battery protection devices; Texas Instruments, 2022). The combination of differentiated protection levels, a bypass path, and a reset enabled by the clearing of all conditions was not found in the sources reviewed, which did not include the internals of proprietary devices; what is offered here is an open, traceable, and simulation-verified description of it. The verification has limits. It relied solely on directed simulation: the 33 successfully verified scenarios establish conformance for each respective case but do not cover the whole domain of inputs. No formal verification techniques, constrained-random methodologies, or coverage metrics have been used. Four plausible edge cases were not run separately, because RTL inspection showed that each uses a branch already covered: repeated toggling of alarms of one category (which triggers the same counter-clear branch of scenario 14), a global reset during counting (triggers the reset branch in scenario 7), manual_reset and rev_pol simultaneously (which engages the same refusing gate exercised by scenario 31), and clearing an alarm as its counter reaches the threshold value (fails the Lockout test and falls through to the Warning and Normal branches of scenarios 16 and 23). Furthermore, the permissive reset was shown through a particular category, which is essentially identical for the others due to the nature of the gate (a single Boolean expression for all categories). One isolated mutation does not suffice to make a judgment about the strength of a testbench; a systematic mutation analysis would give more assurance. Finally, the number of registers utilized is counted from the source and is not a synthesis result, so no information about timing, resources, and power consumption can be claimed. The 3, 7, and 15 cycle thresholds give a relative ordering only.

V. Conclusion

- A four-state Moore-style FSM with independent percategory counters escalates each graded fault on its own schedule, overcurrent fastest and overtemperature slowest (illustrative thresholds of 3, 7 and 15 cycles).
- Reverse polarity bypasses the counters and produced immediate lockout in every state tested; the itel guide lists no fault code for this condition.
- The latch preserves the full fault vector at lockout; manual reset is refused while any condition persists.
- All 33 directed scenarios passed, all 16 transitions were exercised, and a deliberately altered threshold was detected. The evidence comes from simulation only; the design has not been synthesized or built.

VI. Recommendation

Further work should:

1. implement the design on an FPGA, with gate-level timing analysis, resource reporting and validation against a physical charge controller;
2. design and calibrate the sensing front end that supplies the warning and alarm inputs, including input synchronizers;
3. derive thresholds from measured device behavior (switching-device damage curves, battery degradation, thermal mass) once a clock frequency and components are fixed;
4. strengthen verification with coverage-driven or constrained-random testing, formal property checks and a systematic mutation analysis if the design grows; and
5. integrate trip and annunciator with the other cohort subsystems (maximum power point tracking, multistage charging), possibly through a supervisory layer that arbitrates among fault protection, charging strategy and tracking requests, and verify the combined system.

Acknowledgments

During the preparation of this work, the authors used an AI tool (Claude, Anthropic) to assist with drafting and editing the text, drawing diagrams and drafting parts of the Verilog source. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the final version of this publication. All simulations were run by the authors.

References

- [1]. Amin, N., Yi, L.Z., Sopian, K., 2009. Microcontroller based smart charge controller for standalone solar photovoltaic power systems. In: 2009 34th IEEE Photovoltaic Specialists Conference (PVSC). IEEE. doi:10.1109/PVSC.2009.5411210. Bergeron, J., 2003. Writing Testbenches: Functional Verification of HDL Models, 2nd ed. Springer, Boston, MA.
- [2]. IEEE, 2008. IEEE Standard Electrical Power System Device Function Numbers, Acronyms, and Contact Designations. IEEE Std C37.2-2008. IEEE, New York, NY.
- [3]. International Electrotechnical Commission (IEC), 2010a. Functional Safety of Electrical/Electronic/Programmable Electronic SafetyRelated Systems. IEC 61508. IEC, Geneva, Switzerland.
- [4]. International Electrotechnical Commission (IEC), 2010b. Safety of Power Converters for Use in Photovoltaic Power Systems, Part 1: General Requirements. IEC 62109-1. IEC, Geneva, Switzerland.

- [5]. International Electrotechnical Commission (IEC), 2016. Functional Safety, Safety Instrumented Systems for the Process Industry Sector, Part 1: Framework, Definitions, System, Hardware and Application Programming Requirements. IEC 61511-1:2016. IEC, Geneva, Switzerland.
- [6]. International Society of Automation (ISA), 2016. Management of Alarm Systems for the Process Industries. ANSI/ISA-18.2-2016. ISA, Research Triangle Park, NC. itel Energy, n.d. User Guide: Hybrid Inverter (IPV-4K24UPRO, IPV6K48UPRO, IPV-12K48U). User manual.
- [7]. Maheshwari, V., Devulapalli, B.D., Saxena, A.K., 2014. FPGA-based digital overcurrent relay with concurrent sense-process-communicate cycles. *International Journal of Electrical Power & Energy Systems*, 55, 66–73. doi:10.1016/j.ijepes.2013.08.032.
- [8]. Raghavendra, N.K., Padmavathi, K., 2018. Solar charge controller for lithium-ion battery. In: 2018 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), 1–5. doi:10.1109/PEDES.2018.8707743.
- [9]. Shehata, K., Bahaa, A., Hashad, A., 2004a. Design and implementation of an FPGA based protection relay. In: 21st National Radio Science Conference (NRSC 2004). doi:10.1109/NRSC.2004.1321856.
- [10]. Shehata, K., Bahaa, A., Morad, K., Sharaf, A., 2004b. Design and implementation of FPGA based and microcontroller based current relay. In: Proceedings of the 16th International Conference on Microelectronics (ICM 2004), 783–786. doi:10.1109/ICM.2004.1434783.
- [11]. Texas Instruments, 2022. BQ769x0 3-Series to 15-Series Cell Battery Monitor Family for Li-Ion and Phosphate Applications (BQ76920, BQ76930, BQ76940). Data sheet SLUSBK2I, revised March 2022.
- [12]. Texas Instruments, Dallas, TX. <https://www.ti.com/documentviewer/BQ76930/datasheet>
- [13]. Wei, D., Zhang, M., Zhu, L., Chen, H., Huang, W., Yao, J., Yuan, Z., Xu, C., Feng, X., 2022. Study on thermal runaway behavior of Liion batteries using different abuse methods. *Batteries*, 8(11), 201. doi:10.3390/batteries8110201.